

12-21-04

506,908

PCT/DE2003/000761

PATENT COOPERATION TREATY

**PCT****INTERNATIONAL PRELIMINARY EXAMINATION REPORT**

(PCT Article 36 and Rule 70)

Translation

Applicant's or agent's file reference ACDPA5206PWO	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/DE2003/000760	International filing date (<i>day/month/year</i>) 10 March 2003 (10.03.2003)	Priority date (<i>day/month/year</i>) 13 March 2002 (13.03.2002)
International Patent Classification (IPC) or national classification and IPC H04L 9/32		
Applicant DEUTSCHE POST AG		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 15 sheets.

3. This report contains indications relating to the following items:

I Basis of the report

II Priority

III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

IV Lack of unity of invention

V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

VI Certain documents cited

VII Certain defects in the international application

VIII Certain observations on the international application

Date of submission of the demand 02 October 2003 (02.10.2003)	Date of completion of this report 20 September 2004 (20.09.2004)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE2003/000760

I. Basis of the report

1. This report has been drawn on the basis of (Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.):

- the international application as originally filed.
- the description, pages 8-25, as originally filed,
pages _____, filed with the demand,
pages 1-7, 7a, 7b, filed with the letter of 24 August 2004 (24.08.2004),
pages _____, filed with the letter of _____.
- the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-24, filed with the letter of 24 August 2004 (24.08.2004),
Nos. _____, filed with the letter of _____.
- the drawings, sheets/fig 1/3-3/3, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

- the description, pages _____
- the claims, Nos. _____
- the drawings, sheets/fig _____

3. This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/DE 03/00760

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement			
Novelty (N)	Claims	1-24	YES
	Claims		NO
Inventive step (IS)	Claims	1-24	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-24	YES
	Claims		NO

2. Citations and explanations

1. Reference is made to the following documents:

D1: DE 100 20 566 A (POST AG DEUTSCHE)
31 October 2001 (2001-10-31)

D2: DE 100 20 563 A (POST AG DEUTSCHE) 19 April 2001
(2001-04-19) (cited in the application)

2. The application relates to a method for generating counterfeit-proof documents (claim 1) and a value transfer centre with an interface for loading monetary values (claim 23).

D1 discloses a method for providing postal items with franking indicia, wherein there is generated, in the customer system, data encrypted in such a way that a value transfer centre is able to decode it, the data is transmitted from the customer system to the value transfer centre, and the value transfer centre decodes the data, re-encrypts it with a code not known to the customer system and then transmits the encrypted data to the customer system (fig. 4).

D2 discloses a method for generating and checking

counterfeit-proof documents (fig. 1 in the application).

The difference between claims 1 and 23 and the above-mentioned documents lies in the fact that encrypted information from a cryptographically trusted contact point is buffered by an intermediate point (value transfer centre) and is relayed at a separated point in time to a cryptographic module (fig. 3 in the application).

The problem solved by this difference is that of developing a known method so that it can be carried out independently of any direct communication between a cryptographically trusted contact point and a document creator (cryptographic module).

The concept (integration of an untrusted point between the trusted contact point and the document creator) by which the independent claims solve the problem is neither disclosed in nor suggested by the other citations.

The subject matter of claims 1 and 23 is therefore novel and involves an inventive step (PCT Article 33(2) and (3)).

One advantage of the invention is that counterfeit-proof documents can be generated without a data link to the trusted contact point.

Claims 2-22 and 24 are dependent on claims 1 and 23 respectively and therefore likewise satisfy the PCT novelty and inventive step requirements.

**VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM
GEBIET DES PATENTWESEN**

PCT

**INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT
(Artikel 36 und Regel 70 PCT)**

REC'D 21 SEP 2004
WIPO PCT

Aktenzeichen des Anmelders oder Anwalts ACDPA5206PWO	WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/PEA/416)	
Internationales Aktenzeichen PCT/DE 03/00760	Internationales Anmeldedatum (Tag/Monat/Jahr) 10.03.2003	Prioritätsdatum (Tag/Monat/Jahr) 13.03.2002
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04L9/32		
Anmelder DEUTSCHE POST AG et al		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.



2. Dieser BERICHT umfaßt insgesamt 5 Blätter einschließlich dieses Deckblatts.

Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

Diese Anlagen umfassen insgesamt 15 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

- I Grundlage des Bescheids
- II Priorität
- III Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV Mangelnde Einheitlichkeit der Erfindung
- V Begründete Feststellung nach Regel 66.2 a)ii) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI Bestimmte angeführte Unterlagen
- VII Bestimmte Mängel der internationalen Anmeldung
- VIII Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 02.10.2003	Datum der Fertigstellung dieses Berichts 20.09.2004
Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde  Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Apostolescu, R Tel. +49 89 2399-7950 

I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17)*):

Beschreibung, Seiten

8-25 in der ursprünglich eingereichten Fassung
1-7, 7a, 7b eingegangen am 24.08.2004 mit Schreiben vom 18.08.2004

Ansprüche, Nr.

1-24 eingegangen am 24.08.2004 mit Schreiben vom 18.08.2004

Zeichnungen, Blätter

1/3-3/3 in der ursprünglich eingereichten Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um:

- die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- Beschreibung, Seiten:
- Ansprüche, Nr.:
- Zeichnungen, Blatt:

BEST AVAILABLE COPY

5. Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen.)

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung
- | | | |
|--------------------------------|------------------|------|
| Neuheit (N) | Ja: Ansprüche | 1-24 |
| | Nein: Ansprüche | |
| Erfinderische Tätigkeit (IS) | Ja: Ansprüche | 1-24 |
| | Nein: Ansprüche | |
| Gewerbliche Anwendbarkeit (IA) | Ja: Ansprüche: | 1-24 |
| | Nein: Ansprüche: | |

2. Unterlagen und Erklärungen:

siehe Beiblatt

BEST AVAILABLE COPY

Zu Punkt V

Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Es werden folgende Dokumente genannt:

D1: DE 100 20 566 A (POST AG DEUTSCHE) 31. Oktober 2001 (2001-10-31)

D2: DE 100 20 563 A (POST AG DEUTSCHE) 19. April 2001 (2001-04-19) (in der Anmeldung erwähnt)

2. Die Anmeldung betrifft ein Verfahren zur Erstellung fälschungssicherer Dokumente (Anspruch 1) und ein Wertübertragungszentrum mit einer Schnittstelle zum-Laden-von Wertbeträgen (Anspruch 23).

Aus dem Dokument D1 ist ein Verfahren zum Versehen von Postsendungen mit Freimachungsvermerken bekannt, wobei in einem Kundensystem Daten erzeugt werden, die so verschlüsselt sind, daß ein Wertübertragungszentrum diese entschlüsseln kann, daß die Daten von dem Kundensystem zu dem Wertübertragungszentrum gesendet werden und daß das Wertübertragungszentrum die Daten entschlüsselt und anschließend die Daten erneut mit einem dem Kundensystem nicht bekannten Schlüssel codiert und die so verschlüsselten Daten anschließend an das Kundensystem überträgt (Fig. 4).

Aus dem Dokument D2 ist ein Verfahren zur Erstellung und Überprüfung fälschungssicherer Dokumente bekannt (Fig. 1 in der Anmeldung).

Der Unterschied zwischen den Ansprüchen 1 und 23 und den obengenannten Dokumente besteht darin, daß verschlüsselte Informationen einer kryptographisch vertrauenswürdigen Kontaktstelle von einer Zwischenstelle (Wertübertragungszentrum) zwischengespeichert und zeitlich entkoppelt an ein kryptografisches Modul weitergegeben werden (Fig. 3 in der Anmeldung).

Das Problem, das durch diesen Unterschied gelöst wird, ist ein bekanntes Verfahren so weiter zu entwickeln, daß es unabhängig von einer unmittelbaren Kommunikation zwischen einer kryptografisch vertrauenswürdigen Kontaktstelle und einem Dokumenthersteller (kryptografisches Modul) durchgeführt werden kann.

Das Konzept (Einbinden einer nicht vertrauenswürdigen Stelle zwischen der vertrauenswürdigen Kontaktstelle und dem Dokumenthersteller) mit dem die unabhängigen Ansprüche die Aufgabe lösen, ist in den übrigen Druckschriften weder offenbart noch nahegelegt.

Der Gegenstand der Ansprüche 1 und 23 ist somit neu und beruht auf einer erfinderischen Tätigkeit (Artikeln 33 (2) und (3) PCT).

Ein Vorteil der Erfindung besteht darin, daß es möglich ist, fälschungssichere Dokumente ohne eine Datenverbindung zu der vertrauenswürdigen Kontaktstelle zu erstellen.

Die Ansprüche 2-22 und 24 sind vom Anspruch 1 bzw. 23 abhängig und erfüllen damit ebenfalls die Erfordernisse des PCT in bezug auf Neuheit und erfinderische Tätigkeit.

BEST AVAILABLE COPY

**Verfahren zur Erstellung prüfbar fälschungssicherer Dokumente
und Wertübertragungszentrum**

5 Beschreibung:

Die Erfindung betrifft ein Verfahren zur Erstellung fälschungssicherer Dokumente oder Datensätze, wobei eine Schlüsselinformation erzeugt und eine verschlüsselte Prüfinformation aus der Schlüsselinformation und einem Transaktions-Indikator gebildet wird.

Die Erfindung betrifft ferner ein Wertübertragungszentrum mit einer Schnittstelle zum Laden von Wertbeträgen.

15

Es ist eine Vielzahl von Verfahren zur Erzeugung fälschungssicherer Dokumente und zu ihrer Überprüfung bekannt. Übliche Verfahren basieren auf der Erstellung digitaler Signaturen oder verschlüsselter Prüfinformationen, die im Rahmen der Erstellung des Dokuments angefertigt werden.

Zu unterscheiden ist dabei zwischen Dokumenten, bei denen der Ersteller ein Interesse an der Unverfälschtheit hat und solchen, bei denen Dritte ein Interesse an der Unverfälschtheit haben.

25

Hat ein Dritter Interesse an der Fälschungssicherheit von Dokumenten, so ist es bekannt, dass bei der Erstellung des Dokuments ein sogenanntes „kryptografisches Modul“ hinzugezogen wird. Solche bekannten kryptografischen Module zeichnen sich dadurch aus, dass sie in ihrem Inneren elektronische Daten beinhalten oder Daten verarbeiten, die von außen nicht unbe-
merkt eingesehen oder manipuliert werden können.

30

Ein kryptografisches Modul kann als sichere, versiegelte Einheit betrachtet werden, in der sicherheitsrelevante Prozesse durchgeführt werden, die von außen nicht manipuliert werden können. Ein weltweit anerkannter Standard für solche kryptografischen Module ist der von der US-amerikanischen nationalen Behörde für Standardisierung NIST veröffentlichte Standard für kryptografische Module mit der Bezeichnung FIPS Pub 140.

10 Wird zur Erstellung fälschungssicherer Dokumente, an deren Unverfälschtheit Dritte interessiert sind, ein kryptografisches Modul eingesetzt, so besteht eine übliche Realisierung darin, dass das kryptografische Modul genutzt wird, um kryptografische Schlüssel sicher zu hinterlegen, die innerhalb des Moduls, und nur dort, zur Verschlüsselung von Prüfwerten dienen. Bekannt sind beispielsweise sogenannte Signaturkarten, wie sie von Zertifizierungsbehörden oder Trustcentern zur Erstellung von digitalen Signaturen ausgegeben werden. Auch diese Signaturkarten, ausgeführt als Mikroprozessor-Chipkarte, 20 enthalten in eben diesem Mikroprozessor-Chip ein kryptografisches Modul.

In solchen Modulen sind in der Regel ein oder mehrere asymmetrische Schlüsselpaare hinterlegt, die sich dadurch auszeichnen, dass Verschlüsselungen, die mit dem sogenannten privaten Schlüssel erzeugt werden, nur mit dem zugehörigen öffentlichen Schlüssel rückgängig gemacht werden können und dass Verschlüsselungen, die mit dem öffentlichen Schlüssel erzeugt werden, nur mit dem zugehörigen privaten Schlüssel rückgängig gemacht werden können. Gemäß ihrer Bezeichnung sind öffentliche Schlüssel dabei zur Veröffentlichung und beliebigen Verbreitung vorgesehen, wogegen private Schlüssel nicht ausgegeben werden dürfen und bei einer Verwendung zusammen mit kryptografischen Modulen diese Module zu keinem Zeitpunkt ver-

lassen dürfen. Weiterhin hinterlegt in solchen Modulen sind Algorithmen etwa zur Prüfsummenbildung oder, im Beispiel der digitalen Signatur, zur Erstellung eines sogenannten digitalen Fingerabdrucks oder „Hash-Werts“, der sich dadurch auszeichnet, dass er beliebigen Dateninhalt auf eine in der Regel quantitativ deutlich verkürzte Information derart abbildet, dass das Resultat irreversibel und eindeutig ist und dass für verschiedene Dateninhalte, mit denen der Algorithmus gespeist wird, jeweils unterschiedliche Resultate entstehen.

10

Die Erstellung eines fälschungssicheren Dokuments, an dessen Unverfälschtheit Dritte interessiert sind, mittels eines kryptografischen Moduls, das asymmetrische Schlüssel und einen Algorithmus zur Erstellung von Prüfwerten enthält, geschieht üblicherweise wie folgt: Zunächst wird unter Anwendung des Algorithmus zur Erstellung von Prüfwerten ein solcher Prüfwert erstellt, der sich auf das zu sichernde Dokument bezieht. Dann wird ein privater Schlüssel im kryptografischen Modul benutzt, um den Prüfwert zu verschlüsseln. Die Kombination dieser beiden Vorgänge wird als Erstellung einer „digitalen Signatur“ bezeichnet.

15

20

Die Prüfung einer solchen digitalen Signatur geschieht üblicherweise wie folgt: Der Empfänger erhält das Dokument und den verschlüsselten Prüfwert. Der Empfänger benötigt weiterhin, und darauf zielt die später geschilderte Erfindung ab, den öffentlichen Schlüssel des Dokumentherstellers und verwendet diesen zur Entschlüsselung des Prüfwerks, den der Dokumenthersteller mit seinem privaten Schlüssel innerhalb des kryptografischen Moduls verschlüsselt hatte. Nach der Entschlüsselung besitzt der Empfänger somit den unverschlüsselten Prüfwert. Weiterhin wendet der Empfänger im nächsten Schritt den gleichen Algorithmus zur Erstellung eines Prüfwerks auf

25

30

das empfangene Dokument an. Im dritten Schritt schließlich vergleicht der Empfänger den selbst erzeugten Prüfwert mit dem entschlüsselten Prüfwert des Dokumentherstellers. Stimmen beide Prüfwerte überein, so wurde das Dokument nicht verfälscht und die Unverfälschtheit des Dokuments ist zweifelsfrei nachgewiesen. Üblicherweise wird bei bekannten digitalen Signaturen auch die Authentizität des Dokumentherstellers geprüft. Dies geschieht, indem der öffentliche Schlüssel des Dokumentherstellers von einer sogenannten Zertifizierungsstelle oder „CA“ ebenfalls digital signiert und einem bestimmten kryptografischen Modul, beziehungsweise einem bestimmten Inhaber des kryptografischen Moduls, zugeordnet wird. Der Empfänger des Dokuments nimmt in diesem Fall den öffentlichen Schlüssel des Dokumentherstellers nicht einfach als gegeben an; sondern überprüft diesen ebenfalls auf Zugehörigkeit zum Dokumenthersteller, indem er die digitale Signatur des öffentlichen Schlüssels in der oben geschilderten Weise überprüft.

Bei diesen bekannten Verfahren besteht das Problem, dass zur Prüfung der Unverfälschtheit eines Dokuments eine Information erforderlich ist, die unmittelbar mit der Verwendung von Schlüsseln durch den Dokumenthersteller mittels des kryptografischen Moduls zusammenhängt. Im oben angeführten üblichen Beispiel der Erstellung von digitalen Signaturen handelt es sich um den öffentlichen Schlüssel des Dokumentherstellers bzw. dessen kryptografischen Moduls, der zur Prüfung herangezogen werden muss. Im Falle der Signatur des öffentlichen Schlüssels durch eine Zertifizierungsstelle wird das Gesamtgebilde aus öffentlichem Schlüssel, Identifikation des Anwenders dieses Schlüssels sowie der digitalen Signatur der Zertifizierungsstelle als „Schlüsselzertifikat“ bezeichnet.

Zusammengefasst lässt sich diese Problematik an einem Beispiel derart schildern, dass es zur Prüfung der Unverfälschtheit eines üblichen digital signierten Dokuments erforderlich ist, den öffentlichen Schlüssel oder das Schlüsselzertifikat des Dokumentherstellers bzw. seines kryptografischen Moduls bei der Prüfung zur Verfügung zu haben. Sollen an einer Prüfstelle, wie üblich, Dokumente verschiedener Dokumenthersteller geprüft werden, so ist es erforderlich, dort alle öffentlichen Schlüssel oder alle Schlüsselzertifikate aller Dokumenthersteller zur Verfügung zu haben.

Es existieren verschiedene Möglichkeiten, der Anforderung gerecht zu werden, den öffentlichen Schlüssel des Dokumentherstellers bei der Prüfung zur Verfügung zu haben. So ist es möglich, den öffentlichen Schlüssel oder das Schlüsselzertifikat des Dokumentherstellers an das zu sichernde Dokument anzuhängen. Eine weitere Möglichkeit besteht darin, den öffentlichen Schlüssel an der Prüfstelle zu hinterlegen und bei Bedarf auf diesen zuzugreifen.

20

Die bekannten Verfahren sind jedoch mit Nachteilen verbunden.

Das Anhängen des Schlüssels oder des Schlüsselzertifikats ist dann nachteilig, wenn der Umfang des Dokuments möglichst gering gehalten werden muss und ein angehängter Schlüssel den zu druckenden, zu übertragenden oder zu verarbeitenden Datensatz übermäßig vergrößern würde.

Eine Hinterlegung eines öffentlichen Schlüssels an der Prüfstelle ist insbesondere dann nachteilig, wenn ein Zugriff auf an der Prüfstelle hinterlegte Schlüssel aus praktischen oder zeitlichen Erwägungen nicht möglich ist, beispielsweise bei

einer sehr hohen Anzahl von vorgehaltenen Schlüsseln, auf die in sehr kurzer Zeit zugegriffen werden müsste.

Zur Lösung dieser bekannten Nachteile ist es aus der Deutschen Patentschrift DE 100 20 563 C2 der Anmelderin bekannt, bei einem gattungsgemäßen Verfahren in einem Sicherungsmodul ein Geheimnis zu erzeugen, das Geheimnis zusammen mit Informationen, die Auskunft über die Identität des Sicherungsmoduls geben, verschlüsselt an eine Bescheinigungsstelle zu übergeben, das Geheimnis in der Bescheinigungsstelle zu entschlüsseln, hierdurch die Identität des Sicherungsmoduls zu erkennen, anschließend das Geheimnis zusammen mit Informationen zur Identität des Dokumentherstellers derart zu verschlüsseln, dass nur eine Prüfstelle eine Entschlüsselung vornehmen kann, um dann das Geheimnis an einen Dokumenthersteller zu übermitteln. Bei diesem Verfahren gibt der Dokumenthersteller eigene Daten in das Sicherungsmodul ein, wobei das Sicherungsmodul die selbst von dem Dokumenthersteller eingebrachten Daten mit dem Geheimnis irreversibel verknüpft und wobei keine Rückschlüsse auf das Geheimnis möglich sind.

Dieses bekannte Verfahren zeichnet sich dadurch aus, dass das Ergebnis der irreversiblen Verknüpfung der von dem Dokumenthersteller eingebrachten Daten mit dem Geheimnis, die von dem Dokumenthersteller selbst eingebrachten Daten sowie die verschlüsselten Informationen der Bescheinigungsstelle das Dokument bilden, das an die Prüfungsstelle übermittelt wird.

Dieses bekannte Verfahren eignet sich insbesondere zur Erzeugung und Prüfung fälschungssicherer Briefmarken eines Postunternehmens. Solche Briefmarken werden durch Kunden eines Postunternehmens unter Verwendung eines persönlichen kryptografischen Moduls erzeugt und als maschinenlesbarer Barcode auf die

Sendung aufgebracht. Der maschinenlesbare Barcode hat nur einen sehr begrenzten Datenumfang und erlaubt es somit nicht, den öffentlichen Schlüssel des Kunden mit einzubringen. Außerdem müssen in der so genannten Briefproduktion die digitalen Briefmarken in kürzester Zeit gelesen und geprüft werden, wodurch die Möglichkeit, in Sekundenbruchteilen auf eine Datenbasis von möglicherweise vielen Millionen öffentlicher Schlüssel zuzugreifen, ebenfalls entfällt.

10 Ein Verfahren zum Versehen von Postsendungen mit Freimachungsvermerken geht aus der deutschen Offenlegungsschrift DE 100 20 402 A1 der Anmelderin hervor. Bei dem Verfahren werden Informationen, die zum Erstellen eines Freimachungsvermerks von einer Ladestelle verschlüsselt zu einem Kryptomodul eines Kundensystems übertragen, das zur Erzeugung von digitalen Freimachungsvermerken dient. Der Freimachungsvermerk enthält einen Hashwert, der aus den Sendungsdaten und den übertragenen und im Kryptomodul zwischengespeicherten Informationen gebildet wird sowie einen in dieser Information enthaltenen verschlüsselten "Crypto-String", der nur in einem Briefzentrum, bei der Prüfung der Freimachung entschlüsselt werden kann und wird mit einer digitalen Signatur versehen.

25 Die deutsche Offenlegungsschrift DE 100 20 566 A1 der Anmelderin beschreibt ein Verfahren gleicher Art, bei dem Kunden Wertbeträge von einem Wertübertragungszentrum laden können, die zum Ausdrucken von digitalen Freimachungsvermerken verbraucht werden können. Von einem Kundensystem wird dabei insbesondere eine Zufallszahl an das Wertübertragungszentrum übermitteln, das von diesem mit einem symmetrischen Schlüssel verschlüsselt und an das Kundensystem zurückgesandt wird.

7a

Die Erstellung der Freimachungsvermerke wird ebenso durchge-
führt, wie es in der deutschen Offenlegungsschrift
DE 100 20 402 A1 beschrieben ist, wobei die verschlüsselte Zu-
fallszahl insbesondere nur in einem Briefzentrum entschlüsselt
5 werden kann.

Der Erfindung liegt die Aufgabe zugrunde, eine Erstellung von
fälschungssicheren Dokumenten zu ermöglichen, die unabhängig
von einer unmittelbaren Kommunikation zwischen der kryptogra-
10 fisch vertrauenswürdigen Kontaktstelle und dem Dokumenther-
steller durchgeführt werden kann.

Erfindungsgemäße wird diese Aufgabe durch ein Verfahren nach
dem Patentanspruch 1 gelöst.

15

Erfindungsgemäße wird diese Aufgabe ebenfalls durch ein Wert-
übertragungszentrum nach dem Patentanspruch 1 gelöst.

Zweckmäßige Weiterbildung des Verfahrens und des Wertübertra-
20 gungszentrums sind Gegenstand der Unteransprüche.

Die Erfindung sieht insbesondere vor, dass die Erstellung der
zufälligen Schlüsselinformation und die Bildung der verschlüs-
selten Prüfinformation aus der Schlüsselinformation und dem
25 Transaktionsindikator in einer kryptografisch vertrauenswürdigen
Kontaktstelle erfolgen, dass die kryptografisch vertrau-
enswürdige Kontaktstelle die Schlüsselinformation verschlüs-
selt, und dass die verschlüsselte Prüfinformation und die ver-
schlüsselte Schlüsselinformation von der kryptografisch ver-
30 trauenswürdigen Kontaktstelle an eine Zwischenstelle übermit-
telt werden, dass die Zwischenstelle die verschlüsselte
Schlüsselinformation und die verschlüsselte Prüfinformation
zwischenspeichert und zu einem späteren Zeitpunkt zeitlich von

7b

der Übertragung zwischen der kryptografisch vertrauenswürdigen Kontaktstelle und der Zwischenstelle entkoppelt an ein kryptografisches Modul eines Dokumentherstellers übermittelt.

5 Die Erfindung sieht somit vor, dass das kryptografische Modul auch bei einer Speisung über eine Zwischenstelle, beispielsweise über im kryptografischen Sinn nicht vertrauenswürdige Kommunikationspartner mit zwei Arten von Daten versorgt wird, die zum einen im kryptografischen Modul verbleiben und die zum
10 anderen an das Dokument angehängt werden, wobei die im kryptografischen Modul verbleibenden Informationen genutzt werden, um die Dokumentinformationen über einen Prüfwert abzusichern und wobei die in das Dokument übernommenen Informationen dazu
15 dienen, im Rahmen einer Prüfung der Unverfälschtheit des Dokuments in einer Prüfstelle die Absicherung des Dokuments durch das kryptografische Modul nachzuweisen.

Die Erfindung beinhaltet eine Vielzahl von Vorteilen. Sie ermöglicht eine Erzeugung fälschungssicherer Dokumente in einer
20 Vielzahl von Anwendungsfällen, insbesondere bei solchen Fällen, bei denen keine direkte Verbindung zwischen dem Doku

Patentansprüche:

1. Verfahren zur Erstellung fälschungssicherer Dokumente oder Datensätze, wobei eine Schlüsselinformation erzeugt wird und wobei eine verschlüsselte Prüfinformation aus der Schlüsselinformation und einem Transaktionsindikator gebildet wird,
d a d u r c h g e k e n n z e i c h n e t,
dass die Erstellung der zufälligen Schlüsselinformation und die Bildung der verschlüsselten Prüfinformation aus der Schlüsselinformation und dem Transaktionsindikator in einer kryptografisch vertrauenswürdigen Kontaktstelle erfolgen, dass die kryptografisch vertrauenswürdige Kontaktstelle die Schlüsselinformation verschlüsselt, und dass die verschlüsselte Prüfinformation und die verschlüsselte Schlüsselinformation von der kryptografisch vertrauenswürdigen Kontaktstelle an eine Zwischenstelle übermittelt werden, dass die Zwischenstelle die verschlüsselte Schlüsselinformation und die verschlüsselte Prüfinformation zwischenspeichert und zu einem späteren Zeitpunkt zeitlich von der Übertragung zwischen der kryptografisch vertrauenswürdigen Kontaktstelle und der Zwischenstelle entkoppelt an ein kryptografisches Modul eines Dokumentherstellers übermittelt.
2. Verfahren nach Anspruch 1,
d a d u r c h g e k e n n z e i c h n e t,
dass die Schlüsselinformation so erstellt wird, dass die Schlüsselinformation zufällig gebildet wird.
3. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
dass die verschlüsselte Schlüsselinformation und/oder die verschlüsselte Prüfinformation so beschaffen sind, dass sie

in der Zwischenstelle nicht entschlüsselt werden können.

4. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
dass das kryptografische Modul vorzugsweise mit einem in dem kryptografischen Modul enthaltenen Schlüssel eine Entschlüsselung der Schlüsselinformation vornimmt.
5. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
dass der Dokumenthersteller eigene Daten dem kryptografischen Modul übergibt.
6. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
dass das kryptografische Modul die vom Dokumenthersteller eingebrachten Daten mit der Schlüsselinformation irreversibel verknüpft.
7. Verfahren nach Anspruch 6,
d a d u r c h g e k e n n z e i c h n e t,
dass die irreversible Verknüpfung zwischen den von dem Dokumenthersteller eingebrachten Daten und der entschlüsselten Schlüsselinformation dadurch erfolgt, dass unter Verwendung der Schlüsselinformation ein Prüfwert für das Dokument gebildet wird.
8. Verfahren nach einem oder beiden der Ansprüche 6 oder 7,
d a d u r c h g e k e n n z e i c h n e t,
dass das Ergebnis der irreversiblen Verknüpfung der von dem

Dokumenthersteller eingebrachten Daten mit der entschlüsselten Schlüsselinformation ein Dokument und/oder einen Datensatz bilden, der an eine Prüfstelle übermittelt wird.

9. Verfahren nach Anspruch 8,
dadurch gekennzeichnet,
dass das an die Prüfstelle übermittelte Dokument die von dem Dokumenthersteller eingebrachten eigenen Daten wenigstens teilweise im Klartext enthält.
10. Verfahren nach einem oder beiden der Ansprüche 8 oder 9,
dadurch gekennzeichnet,
dass in das an die Prüfstelle übermittelte Dokument die verschlüsselte Prüfinformation eingebracht wird.
11. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche,
dadurch gekennzeichnet,
dass in dem kryptografischen Modul Informationen verbleiben, die derart verschlüsselt sind, dass sie im kryptografischen Modul entschlüsselt werden können.
12. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche,
dadurch gekennzeichnet,
dass die Versorgung des kryptografischen Moduls mit den Informationen auch bei einer Speisung über im kryptografischen Sinne nicht vertrauenswürdige Kommunikationspartner durch eine kryptografisch vertrauenswürdige Stelle erfolgt, auf deren Information sich die Prüfstelle verlassen kann.
13. Verfahren nach Anspruch 12,
dadurch gekennzeichnet,

dass zur Bereitstellung vertrauenswürdiger Informationen für das kryptografische Modul durch eine vertrauenswürdige Stelle kryptografische Verschlüsselungen angewendet werden, die die Prüfstelle rückgängig machen kann.

14. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
dass die Versorgung des kryptografischen Moduls über kryptografisch nicht vertrauenswürdige Kommunikationspartner derart erfolgt, dass die Weiterreichung der Informationen an das kryptografische Modul zeitlich entkoppelt ist.
15. Verfahren nach einem oder mehreren der Ansprüche 1 bis 14,
d a d u r c h g e k e n n z e i c h n e t,
dass die Versorgung des kryptografischen Moduls über kryptografisch nicht vertrauenswürdige Kommunikationspartner derart erfolgt, dass ein Austausch von Informationen innerhalb eines Dialogs nicht erforderlich ist.
16. Verfahren nach einem oder mehreren der Ansprüche 1 bis 14,
d a d u r c h g e k e n n z e i c h n e t,
dass die beiden Arten von Daten kryptografisch miteinander verknüpft sind, jedoch nicht auf dem Wege der Kryptoanalyse aufgedeckt werden.
17. Verfahren nach Anspruch 16,
d a d u r c h g e k e n n z e i c h n e t,
dass die kryptografische Verknüpfung der beiden Arten von Daten dergestalt ist, dass nicht lineare Anteile, die nur der vertrauenswürdigen Kontaktstelle und der Prüfstelle bekannt sind, hinzugefügt werden.

18. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche,
dadurch gekennzeichnet,
dass die erstellten fälschungssicheren Dokumente oder Datensätze Geldwertinformationen enthalten.
19. Verfahren nach 18,
dadurch gekennzeichnet,
dass die Geldwertinformation kryptografisch mit dem Dokument oder dem Datensatz derart verbunden ist, dass durch einen Vergleich zwischen den Geldwertinformationen und dem Dokument oder den Datensatz ein Prüfwert gebildet werden kann.
20. Verfahren nach einem oder beiden der Ansprüche 18 oder 19,
dadurch gekennzeichnet,
dass die Geldwertinformationen einen Nachweis über die Entrichtung von Portobeträgen enthalten.
21. Verfahren nach Anspruch 20,
dadurch gekennzeichnet,
dass die den Entrichtung des Portobetrag nachweisenden geldwerter Informationen mit Identifikationsangaben des Dokumentherstellers verknüpft sind.
22. Verfahren nach einem oder beiden der Ansprüche 20 oder 21,
dadurch gekennzeichnet,
dass die geldwerten Informationen mit einer Adressangabe verknüpft werden.

23. Wertübertragungszentrum mit einer Schnittstelle zum Laden von Wertbeträgen,

d a d u r c h g e k e n n z e i c h n e t,

dass das Wertübertragungszentrum eine Schnittstelle zum Empfang von verschlüsselten Informationen einer kryptografisch vertrauenswürdigen Kontaktstelle und zur Zwischenspeicherung der empfangenen verschlüsselten Informationen sowie Mittel für einen Empfang von Wertübertragungsaufforderungen durch wenigstens ein kryptografisches Modul und zur zeitlich entkoppelten Weitergabe der erhaltenen verschlüsselten Information an das kryptografische Modul enthält.

24. Wertübertragungszentrum nach Anspruch 23,

d a d u r c h g e k e n n z e i c h n e t,

dass die Informationen so verschlüsselt sind, dass sie in dem Wertübertragungszentrum nicht entschlüsselt werden können.